Google Cloud

Professional Cloud Network Engineer

認定試験ガイド

プロフェッショナル クラウド ネットワーク エンジニアは、Google Cloud ネットワーク インフラストラクチャの設計、実装、管理を担当します。これには、高可用性、スケーラビリティ、レジリエンス、セキュリティを考慮したネットワーク アーキテクチャの設計が含まれます。また、Virtual Private Cloud（VPC）、ルーティング、ネットワーク セキュリティ サービス、ロード バランシング、Cloud NAT、Cloud DNS の構成と管理に精通しており、Cloud Interconnect と Cloud VPN を介したハイブリッド接続とマルチクラウド接続の設定にも習熟しています。専門知識の範囲は、Google Cloud Observability と Network Intelligence Center を使用したネットワーク運用の診断、モニタリング、トラブルシューティングにまでおよびます。

セクション **1: Google Cloud Virtual Private Cloud**（**VPC**）ネットワークの設計と計画（試験内容の約 **24%**）

1.1 全体的なネットワーク アーキテクチャを設計する。以下のような点を考察します。

- 高可用性、フェイルオーバー、障害復旧、スケールを考慮した設計。
- DNS トポロジの設計（オンプレミス、Cloud DNS など）。
- アプリケーションまたはソリューション用のロードバランサの選択。
- ハイブリッド接続を考慮した設計（ハイブリッド接続用のプライベート Google アクセスなど）。
- Google Kubernetes Engine（GKE）ネットワーキングに向けた計画（セカンダリ範囲、IP アドレス空間に基づくスケーリングの可能性、GKE コントロール プレーンへのアクセスなど）。
- Identity and Access Management（IAM）ロールの計画（共有 VPC 環境での IAM ロールの管理など）。
- マネージド サービスへの接続に向けた計画（プライベート サービス アクセス、Private Service Connect、サーバーレス VPC アクセスなど）。
- 異なるネットワーク ティア（プレミアムとスタンダードなど）の区別。

1.2 VPC ネットワークを設計する。以下のような点を考察します。

- VPC のタイプと数量の選択（スタンドアロン VPC または共有 VPC、VPC 環境の数など）。
- 要件に基づくネットワーク相互接続方法の決定（VPC ネットワーク ピアリング、Network Connectivity Center によるネットワーク接続（メッシュ トポロジとスタートポロジ）、Private Service Connect など）。

- IP アドレス管理戦略の計画（サブネット、IPv6、お客様所有 IP の使用（パブリック アドバタイズド プレフィックス（PAP）とパブリック委任プレフィックス（PDP））、Private NAT、RFC 1918 以外、マネージド サービスなど）。
- グローバルまたはリージョン（またはこれらのバリエーション）のネットワーク環境の計画。
- ワークロードの VPC に適した MTU サイズの決定。
- カスタム ルート（静的またはポリシーベース）とロード バランシングを使用したサードパーティ製デバイス（ネットワーク仮想アプライアンスなど）の挿入計画。

1.3 復元力とパフォーマンスに優れたハイブリッドおよびマルチクラウド ネットワークを設計する。以下のような点を考察します。

- 帯域幅とセキュリティの制約を含むハイブリッド（オンプレミスとクラウド、支店）接続を考慮した設計（Dedicated Interconnect、Partner Interconnect、Cloud VPN、SD-WAN アプライアンスなど）。
- マルチクラウド接続を考慮した設計（Cloud VPN、Cross-Cloud Interconnect など）。
- ダイレクト ピアリングと Verified Peering Provider の使い分け。
- 複数のリージョンを対象とした高可用性と障害復旧を考慮した接続戦略の設計（リージョンまたはグローバルの動的ルーティング モードなど）。
- オンプレミス ロケーションから複数の VPC へのアクセス（共有 VPC、マルチ VPC ピアリング、Network Connectivity Center トポロジなど）。
- オンプレミス ロケーションから Vertex AI などの Google サービスや API へのプライベート アクセス（Google API 用の Private Service Connect など）。
- Private Service Connect（PSC）または VPC ネットワーク ピアリング接続（プライベート サービス アクセス、サービス ネットワーキングなど）を介したマネージド サービスへのアクセス。
- オンプレミス ロケーションとクラウド環境にまたがる IP アドレス空間の設計（内部範囲、重複回避のための計画など）。
- DNS ピアリングおよび転送戦略の設計（DNS 転送パスなど）。
- ワークロードのハイブリッド接続（Cloud Interconnect と HA VPN）に適した MTU サイズの決定。
- Cloud Interconnect を介した MACsec や HA VPN などのインターコネクト暗号化オプションについての理解。

1.4 Google Kubernetes Engine（GKE）を設計する。以下のような点を考察します。

- クラスタノードとノードプールをパブリックとプライベートのどちらにするかの選択。
- コントロール プレーン エンドポイントをパブリックとプライベートのどちらにするかの選択。
- サブネットの計画: プライマリ範囲とセカンダリ範囲。
- RFC 1918、RFC 1918 以外、プライベートで使用されるパブリック IP（PUPI）アドレスのいずれにするかの選択。
- IPv6 に向けた計画。
- GKE ネットワーキングのロード バランシングの設計。

- ノードプールの構成の追加と管理。

セクション 2: VPC ネットワークの実装（試験内容の約 19%）

2.1 VPC を構成する。以下のような点を考察します。

- Google Cloud VPC リソースの作成（ネットワーク、サブネット、ファイアウォール ルールまたはポリシー、プライベート サービス アクセスのサブネット、プライベート プールなど）。
- VPC ネットワーク ピアリングの構成。
- 共有 VPC ネットワークの作成と他のプロジェクトとのサブネットの共有。
- Google API と Google マネージド サービス（プライベート Google アクセス、パブリック インターフェースなど）へのアクセスの構成。
- Vertex AI サービスへのアクセスの構成。
- 作成後の VPC サブネット範囲の拡大。
- VPC Service Controls の境界を使用した制限付きの Google Cloud サービスの構成。

2.2 VPC ルーティングを構成する。以下のような点を考察します。

- 静的ルーティングと動的ルーティング（Cloud Router など）の設定。
- グローバルまたはリージョンの動的ルーティングの構成。
- ネットワーク タグと優先度を使用したルーティングの実装。
- グローバル動的ルーティングでのルートの優先度の設計。
- ネクストホップとしての内部ロードバランサの実装。
- VPC ネットワーク ピアリングを介したカスタム ルートのインポートとエクスポートの構成。
- ポリシーベース ルーティングの構成。

2.3 Network Connectivity Center を構成する。以下のような点を考察します。

- スポークタイプ（VPC スポーク、ハイブリッド スポーク、プロデューサー スポーク）の区別。
- VPC トポロジの管理（スタートポロジ、ハブ アンド スポーク、メッシュ トポロジなど）。
- Private NAT と Private Service Connect の伝播の構成。
- NCC スポークの IP / CIDR の範囲フィルタの構成。
- NCC のモニタリングとトラブルシューティング。

2.4 Google Kubernetes Engine クラスタの構成と保守を行う。以下のような点を考察します。

- エイリアス IP を使用した VPC ネイティブ クラスタの作成。
- 共有 VPC を使用したクラスタの設定。
- プライベート クラスタとコントロール プレーンのプライベート エンドポイントの構成。

- クラスタ コントロール プレーン エンドポイント用の承認済みネットワークの追加。
- GKE Dataplane V2 の有効化。
- 送信元 NAT（SNAT）ポリシーと IP マスカレード ポリシーの構成。
- GKE ネットワーク ポリシーの作成。
- Pod 範囲と Service 範囲の構成。
- GKE クラスタへの追加の Pod 範囲のデプロイ。

セクション **3:** マネージド ネットワーク サービスの構成（試験内容の約 **21%**）

3.1 ロード バランシングを構成する。以下のような点を考察します。

- ネットワークのロード バランシング ソリューションの決定（内部 / 外部、リージョン / グローバル、アプリケーション / プロキシ / パススルーなど）。
- バックエンド サービスの構成（ネットワーク エンドポイント グループ（NEG）、マネージド インスタンス グループなど）。
- 分散方式、セッション アフィニティ、処理能力、URL マップ、ヘルスチェック、グローバル アクセスなど、さまざまなロードバランサとバックエンドの設定の構成。
- 自動スケーリング機能または手動スケーリング機能を使用した、トラフィックのスケーラビリティの最適化。
- GKE のロードバランサ（GKE Gateway Controller、GKE Ingress コントローラ、NEG など）の理解。
- アプリケーション ロードバランサでのトラフィック管理の設定（トラフィック分割、トラフィックのミラーリング、URL の書き換えなど）。

3.2 Cloud CDN を構成する。以下のような点を考察します。

- 対応している送信元（マネージド インスタンス グループ、Cloud Storage バケット、Cloud Run など）用の Cloud CDN の設定。
- 外部バックエンド（インターネット NEG）とサードパーティのオブジェクト ストレージ用の Cloud CDN の設定。
- キャッシュに保存されたコンテンツの無効化。
- 署名付き URL の構成。

3.3 Cloud DNS を構成する。以下のような点を考察します。

- Cloud DNS のゾーンとレコードの管理。
- Cloud DNS への移行。
- 位置情報ポリシーやフェイルオーバー ポリシーなどの Cloud DNS ルーティング ポリシーの構成。

- DNS Security Extensions（DNSSEC）の有効化。
- DNS 転送と DNS サーバーのポリシー構成など、Cloud DNS とセルフホスト DNS の統合の設定。
- DNS のプライベート ゾーンとパブリック ゾーンの理解と、スプリット ホライズン DNS の設定。
- DNS のプロジェクト間バインディングと DNS ピアリングの設定。
- GKE 用の Cloud DNS と外部 DNS オペレーターの構成。

セクション **4:** ハイブリッドおよびマルチクラウド ネットワークの相互接続の構成と実装（試験内容の約 **15%**）

4.1 Cloud Interconnect を構成する。以下のような点を考察します。

- Dedicated Interconnect 接続の作成と VLAN アタッチメントの構成。
- Partner Interconnect 接続の作成、VLAN アタッチメントの構成、レイヤ 2 タイプとレイヤ 3 タイプの Partner Interconnect の区別。
- Cross-Cloud Interconnect 接続の作成と VLAN アタッチメントの構成。
- Cloud Interconnect を介した HA VPN の構成。
- Interconnect トポロジへの 99.9% SLA と 99.99% SLA の実装。

4.2 サイト間 IPsec VPN を構成する。以下のような点を考察します。

- オンプレミス VPN ゲートウェイに接続する HA VPN の構成。
- 他の Google Cloud VPC に接続する HA VPN の構成。
- Classic VPN の構成（ルートベース、ポリシーベースなど）。

4.3 Cloud Router を構成する。以下のような点を考察します。

- Border Gateway Protocol（BGP）属性の実装（ASN、ルート優先度 / MED、リンクローカル アドレス、認証など）。
- Bidirectional Forwarding Detection（BFD）の構成。
- カスタム アドバタイズ ルートとカスタムの学習したルートの作成。
- VPC での最適パス選択モードの選択（標準モードまたは従来モード）。

4.4 Network Connectivity Center を構成する。以下のような点を考察します。

- ハイブリッド スポークの作成（VPN、VLAN アタッチメントなど）。
- サイト間データ転送の確立。
- ルーター アプライアンス（RA）の作成。
- 一般的なトランジット ネットワークの問題の解決。

セクション **5:** ネットワーク オペレーションの管理、モニタリング、トラブルシューティング（試験内容の約 **13%**）

5.1 ロギングとモニタリングに Google Cloud Observability を使用する。以下のような点を考察します。

- ネットワーキング コンポーネント（Cloud VPN、Cloud Router、VPC Service Controls、Cloud NGFW、ファイアウォール インサイト、VPC フローログ、Cloud DNS、Cloud NAT、NCC など）における Cloud Logging の有効化と確認。
- ネットワーク指標のモニタリング（Cloud VPN、Cloud Interconnect、VLAN アタッチメント、Cloud Router、ロードバランサ、Google Cloud Armor、Cloud NAT など）。

5.2 接続の維持管理とその問題のトラブルシューティングを行う。以下のような点を考察します。

- アプリケーション ロードバランサを使用した、トラフィック フローのドレインとリダイレクト。
- VPN の管理とトラブルシューティング。
- Cloud Interconnect の問題の管理とトラブルシューティング。
- Cloud Router の BGP ピアリングの問題のトラブルシューティング。
- VPC フローログ、ファイアウォール ログ、Packet Mirroring を使用したトラブルシューティング。

5.3 Network Intelligence Center を使用した、ネットワークに関する一般的な問題のモニタリングとトラブルシューティングを行う。以下のような点を考察します。

- ネットワーク トポロジを使用した、スループットとトラフィック フローの可視化。
- 接続テストを使用した、ルートおよびファイアウォールの構成ミスの診断。
- パフォーマンス ダッシュボードを使用した、パケットロスとレイテンシの特定（Google 全体、プロジェクト スコープなど）。
- ファイアウォール インサイトを使用した、ルールのヒット数のモニタリングとシャドウルールの特定。
- ネットワーク アナライザを使用した、ネットワーク障害、最適ではない構成、使用率に関する警告の特定。
- Flow Analyzer と VPC フローログを使用した、ネットワーク トラフィックの評価。

セクション **6:** クラウド ネットワーク セキュリティ ソリューションの構成、実装、管理（試験内容の約 **14%**）

6.1 Google Cloud Armor ポリシーを構成する。以下のような点を考察します。

- エッジとバックエンドのセキュリティ ポリシーの構成とアタッチ。

- ウェブ アプリケーション ファイアウォール（WAF）ルールの実装（SQL インジェクション、クロスサイト スクリプティング、リモート ファイル インクルードなど）。
- 高度なネットワーク分散型サービス拒否攻撃（DDoS）と Adaptive Protection の構成。
- レート制限の構成。
- bot 管理の構成。
- Google Threat Intelligence の適用。

6.2 Cloud Next Generation Firewall（NGFW）ポリシーと VPC ファイアウォール ルールを構成、管理する。以下のような点を考察します。

- ファイアウォール戦略の計画（VPC ファイアウォール ルール、Cloud Next Generation Firewall、階層型ファイアウォール ルール、サードパーティ統合など）。
- GKE と Cloud ロードバランサをサポートするための Cloud NGFW の構成。
- VPC Cloud ファイアウォール ルールと Cloud NGFW リージョン / グローバル / 階層型ポリシーの作成とトラブルシューティング。
- Cloud NGFW Enterprise でのレイヤ 7 パケット検査の有効化。
- VPC ファイアウォール ルールから Cloud NGFW ポリシーへの移行。
- VPC と NGFW のルール条件の構成（ルールの優先度、ネットワーク プロトコル、方向（上り（内向き）と下り（外向き））、送信元、宛先など）、VPC とファイアウォール ルールのロギングの構成。
- セキュリティ目的でのマイクロセグメンテーションの組み込み（メタデータ、（セキュア）タグ、サービス アカウント、ネットワーク タグの使用など）。
- Cloud NGFW のさまざまなティア（Essentials、Standard、Enterprise）の区別。

6.3 パブリック Cloud NAT と Secure Web Proxy を使用してインターネット下り（外向き）トラフィックを構成して保護する。以下のような点を考察します。

- パブリック Cloud NAT IP アドレスの構成、自動および手動による NAT IP アドレスの割り当て。
- Cloud NAT の静的ポート割り当てと動的ポート割り当ての構成。
- Secure Web Proxy の構成。

6.4 セルフマネージドのネットワーク パケット インスペクション、IDS、Packet Mirroring を構成する。以下のような点を考察します。

- マルチ NIC VM（NGFW アプライアンスなど）を使用した VPC 間トラフィックのルーティングと検査。
- 高可用性マルチ NIC VM ルーティングのネクストホップとしての内部ロードバランサの構成。
- 高可用性マルチ NIC VM ルーティングのポリシーベース ルートの構成。
- アウトオブバンドの Network Security Integration（NSI）の戦略の策定。
- Cloud Intrusion Detection System（IDS）の構成。
- 自己管理コレクタに向かう VPC トラフィックの Packet Mirroring の構成。